Anforderungen an die Informationssicherheit

1. Einführung

Der Anbieter und CWT haben eine Vereinbarung getroffen, in deren Rahmen sich der Anbieter bereit erklärt hat, Dienstleistungen und/oder Produkte gemäß den Bedingungen dieser Vereinbarung („**Vereinbarung**“) bereitzustellen. Der Anbieter erklärt sich damit einverstanden, dass er die in diesem Dokument enthaltenen Informationssicherheitsanforderungen („**Informationssicherheitsanforderungen**“) und die erforderlichen Informationssicherheitsmaßnahmen („**technische und organisatorische Sicherheitsmaßnahmen“**) einhält und in seinem Namen handelnde Dritte dazu veranlasst, diese einzuhalten . Die Anforderungen an die Informationssicherheit und die technischen und organisatorischen Sicherheitsmaßnahmen werden in die Vereinbarung aufgenommen und zu einem Bestandteil dieser Vereinbarung gemacht.

2. Definitionen

2.1 Sofern hierin nicht anders angegeben oder erweitert, haben definierte Begriffe die gleiche Bedeutung wie in der Vereinbarung festgelegt. Die folgenden definierten Begriffe gelten für diese Informationssicherheitsanforderungen . Im Falle eines Widerspruchs zwischen der in der Vereinbarung enthaltenen Definition und der hierin enthaltenen Definition gilt die Definition in diesem Dokument in Bezug auf die Informationssicherheitsanforderungen.

„**Verbundene Unternehmen**“, sofern in der Vereinbarung nicht anders definiert, bedeutet in Bezug auf eine Partei jedes Unternehmen oder jede andere juristische Person, die zum Datum der Unterzeichnung der Vereinbarung direkt oder indirekt: (i) eine Partei kontrolliert; oder (ii) von einer Partei kontrolliert wird; oder (iii) von einem Unternehmen oder einer juristischen Person kontrolliert wird, die eine Partei direkt oder indirekt kontrolliert. Für diese Zwecke bedeutet „Kontrolle“ das Recht, mehr als fünfzig Prozent (50%) der Stimmrechte oder ähnlichen Eigentumsrechte auszuüben; aber nur so lange, wie eine solche Kontrolle bestehen bleibt.

„**Autorisierter Mitarbeiter**“ bezeichnet die Mitarbeiter des Anbieters, die vertrauliche Informationen und personenbezogene Daten kennen oder anderweitig darauf zugreifen müssen, damit der Anbieter seine Verpflichtungen aus der Vereinbarung erfüllen kann.

„**Autorisierte Partei**“ oder **„autorisierte Parteien**“ bezeichnet die (i) autorisierten Mitarbeiter des Anbieters; und (ii) Dritte, die personenbezogene Daten und vertrauliche Informationen kennen oder anderweitig darauf zugreifen müssen, damit der Anbieter seine Verpflichtungen im Rahmen der Vereinbarung erfüllen kann, und die schriftlich an Vertraulichkeits- und andere Verpflichtungen gebunden sind, die ausreichen , um personenbezogene Daten und vertrauliche Informationen zu schützen in Übereinstimmung mit den Bedingungen der Vereinbarung und diesem Dokument .

„**Vertrauliche Informationen**“ bezeichnet alle wirtschaftlich sensiblen, geschützten oder anderweitig vertraulichen Informationen in Bezug auf (a) CWT, seine Partner und seine verbundenen Unternehmen; (b) einem CWT-Kunden und Mitarbeitern, Auftragnehmern,

Subunternehmern oder Lieferanten von CWT-Kunden; (c) CWT-Personal; (d) seine unabhängigen Partner und Joint Venturer; oder (e) den Inhalt und/oder Zweck der Vereinbarung, ob mündlich, schriftlich oder auf andere Weise, die direkt oder indirekt in den Besitz des Verkäufers oder in den Besitz autorisierter Parteien als Ergebnis oder im Zusammenhang mit der gelangen können Zustimmung. Zur Klarstellung: Alle Arbeitsergebnisse stellen vertrauliche Informationen dar.

„**CWT** , sofern in der Vereinbarung nicht anders definiert, bedeutet das in der Vereinbarung beschriebene CWT-Unternehmen sowie seine verbundenen Unternehmen.

„**Demilitarisierte Zone**“ oder „**DMZ**“ ist ein Netzwerk oder Teilnetzwerk, das sich zwischen einem vertrauenswürdigen internen Netzwerk wie einem privaten lokalen Netzwerk (LAN) eines Unternehmens und einem nicht vertrauenswürdigen externen Netzwerk wie dem öffentlichen Internet befindet. Eine DMZ verhindert, dass externe Benutzer direkten Zugriff auf interne Systeme und andere Ressourcen erhalten.

„**Vorfallmanagementprozess**“ ist ein vom Anbieter entwickelter, dokumentierter Prozess und ein Verfahren, das im Falle eines tatsächlichen oder mutmaßlichen Angriffs, Eindringens, unbefugten Zugriffs, Verlusts oder einer anderen Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität zu befolgen ist von personenbezogenen Daten und vertraulichen Informationen von CWT.

„**Maskieren**“ ist der Vorgang des Abdeckens von Informationen, die auf einem Bildschirm angezeigt werden.

„**Mobile und tragbare Geräte**“ bezeichnet mobile und/oder tragbare Computer, Geräte, Medien und Systeme, die leicht getragen, bewegt, transportiert oder übermittelt werden können und die im Zusammenhang mit der Vereinbarung verwendet werden. Beispiele für solche Geräte sind Laptops, Tablets, USB-Festplatten, USB-Speichersticks, Personal Digital Assistants (PDAs), Mobil- oder Datentelefone und alle anderen drahtlosen, Peripherie- oder Wechselgeräte mit der Fähigkeit, vertrauliche Informationen und persönliche Informationen zu speichern .

„**Personenbezogene Daten**“, sofern in der Vereinbarung nicht anders definiert, bedeutet im Sinne der Verordnung (EU) 2016/679 und anderer anwendbarer globaler Informationssicherheits-, Datenschutz- und Datenschutzgesetze alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, die sein kann direkt oder indirekt identifiziert werden, insbesondere durch Bezugnahme auf eine Identifikationsnummer oder auf einen oder mehrere Faktoren, die für seine physische, physiologische, geistige, wirtschaftliche, kulturelle oder soziale Identität spezifisch sind. Personenbezogene Daten sind Eigentum von CWT, nicht des Anbieters.

„**Sicherheits-Gateway**“ bezeichnet eine Reihe von Kontrollmechanismen zwischen zwei oder mehr Netzwerken mit unterschiedlichen Vertrauensstufen, die den zwischen Netzwerken und den zugehörigen Verwaltungs- und Verwaltungsservern passierenden oder zu passieren versuchten Datenverkehr filtern und protokollieren. Beispiele für Sicherheits-Gateways sind

Firewalls, Firewall-Management-Server, Hop-Boxen, Session Border Controller, Proxy-Server und Intrusion-Prevention-Geräte.

„**Starke Authentifizierung**“ bedeutet die Verwendung von Authentifizierungsmechanismen und Authentifizierungsmethoden, die mehrere Authentifizierungsfaktoren erfordern, einschließlich mindestens zwei der folgenden: (1) Wissen – etwas, das der Benutzer weiß, z . B. Passwort oder persönliche Identifikationsnummer, (2) Eigentum – etwas der Benutzer hat zB einen Token, eine Chipkarte, ein Mobiltelefon und (3) Inhärenz – etwas, das der Benutzer ist, zB ein Fingerabdruck.

„**Starke Verschlüsselung**“ bedeutet die Verwendung von Verschlüsselungstechnologien mit einer Mindestschlüssellänge von 256 Bit für symmetrische Verschlüsselung und 1024 Bit für asymmetrische Verschlüsselung, deren Stärke hinreichende Gewähr dafür bietet, dass sie die verschlüsselten Informationen vor unbefugtem Zugriff schützt und angemessen ist, um die Vertraulichkeit zu wahren und Vertraulichkeit der verschlüsselten Informationen , und die eine dokumentierte Richtlinie für die Verwaltung der Verschlüsselungsschlüssel und zugehöriger Prozesse enthält, die angemessen sind, um die Vertraulichkeit und Vertraulichkeit der Schlüssel und Passwörter zu schützen, die als Eingaben für den Verschlüsselungsalgorithmus verwendet werden. Starke Verschlüsselung beinhaltet, ist aber nicht beschränkt auf: SSL v3.0+/TLS v1.2, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (nur Regierung der Vereinigten Staaten), RSA 1024 Bit, SHA1/SHA2 /SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 oder WPA2.

„**Technische und organisatorische Sicherheitsmaßnahmen**“ bezeichnet alle Aktivitäten, die gemäß diesen Informationssicherheitsanforderungen erforderlich sind um auf Informationen oder Daten zuzugreifen, diese zu verwalten, zu übertragen, zu verarbeiten, zu speichern, aufzubewahren und zu vernichten; um betroffene Parteien offenzulegen und zu benachrichtigen, die gemäß der Vereinbarung und den geltenden Datenschutz- und Datenschutzgesetzen erforderlich sind; und Informationen oder Daten zu schützen, um Verfügbarkeit, Integrität, Vertraulichkeit und Datenschutz zu gewährleisten, oder Einzelpersonen über ein Versäumnis zu informieren, solche Informationen oder Daten zu schützen. Zu den Maßnahmen gehören unter anderem diejenigen, die gemäß der EU-Datenschutz-Grundverordnung (DSGVO), der EU-Zahlungsdienstrichtlinie, dem California Consumer Privacy Act, NYS DFS 23 NYCRR 500 , dem United States Gramm-Leach Bliley Act (GLBA), dem United States Health Insurance Portability and Accountability Act (HIPAA), den Datenschutzanforderungen der EU/Schweiz und allen anderen internationalen und US-Gesetzen, offiziellen Rechtsauslegungen oder Präzedenzfällen in Bezug auf Informationen oder Daten im Rahmen der Vereinbarung .

„**Dritter**“ oder „**Dritte**“ bedeutet Anbieter Subunternehmer , Berater, Zeitarbeitskräfte, Auftragnehmer oder zusätzliche Anbieter und/oder Vertreter, die im Namen des Anbieters handeln, und umfasst jede Definition von Drittanbietern nach geltendem EU-, US- oder anderem internationalen Recht.

„**Anbieter**“ bezeichnet die in der Vereinbarung festgelegte Vertragspartei zusammen mit ihren verbundenen Unternehmen und ihren Drittparteien.

3 . Organisation der Informationssicherheit

Der Anbieter muss mindestens :

3.1 Stellen Sie sicher, dass nur autorisierten Parteien Zugriff auf personenbezogene Daten und vertrauliche Informationen gewährt wird.

3.2 Implementieren Sie technische und organisatorische Sicherheitsmaßnahmen, die nicht weniger streng sind als Best Practices für die Informationssicherheit, um die Integrität, Verfügbarkeit und Vertraulichkeit vertraulicher Informationen, personenbezogener Informationen und anderer nicht öffentlicher Informationen zu schützen und den unbefugten Zugriff, Erwerb, Offenlegung, Zerstörung und Änderung zu verhindern , versehentlicher Verlust, Missbrauch oder Beschädigung der persönlichen Daten oder vertraulichen Informationen.

3.3 Etablieren, implementieren und pflegen Sie im Einklang mit bewährten Verfahren der Branche, Richtlinien und einem Programm organisatorischer, betrieblicher, administrativer, physischer und technischer und organisatorischer Sicherheitsmaßnahmen, die geeignet sind, um (1) jeglichen Zugriff durch nicht autorisierte Parteien auf personenbezogene Daten und vertrauliche Informationen zu verhindern auf eine Weise, die nicht durch die Vereinbarung oder diese Informationssicherheitsanforderungen autorisiert ist, und (2) alle anwendbaren Gesetze und Vorschriften und anwendbaren Industriestandards einhalten und einhalten.

3.4 Bieten Sie autorisierten Parteien, die Zugriff auf personenbezogene Daten und vertrauliche Informationen haben , Überwachung, Anleitung und Schulung zu den technischen und organisatorischen Sicherheitsmaßnahmen an, einschließlich Schulungen, die praktische Übungen bieten, die auf aktuelle Bedrohungsszenarien abgestimmt sind, und den Teilnehmern Feedback geben . Der Anbieter muss bei der Einstellung eines autorisierten Mitarbeiters und vor dem Zugriff einer autorisierten Partei auf vertrauliche Informationen und personenbezogene Daten Schulungen zu technischen und organisatorischen Sicherheitsmaßnahmen anbieten. Eine Auffrischungsschulung muss mindestens jährlich und so bald wie möglich nach jeder wesentlichen Änderung der technischen und organisatorischen Sicherheitsmaßnahmen des Anbieters durchgeführt werden.

3.5 Bieten Sie spezialisierte Schulungen speziell für autorisierte Parteien mit erheblichen Sicherheitsaufgaben an, einschließlich, aber nicht beschränkt auf Personal- oder Informationstechnologiefunktionen und alle Funktionen von Technologieadministratoren. Die spezialisierte Schulung umfasst mindestens, je nach Funktion, Informationssicherheitsverfahren, akzeptable Nutzung von Informationssicherheitsressourcen, aktuelle Bedrohungen für Informationssysteme, Sicherheitsfunktionen bestimmter Systeme und sichere Zugriffsverfahren.

3.6 Ergreifen Sie angemessene Maßnahmen, um den unbefugten Zugriff auf oder den Verlust von personenbezogenen Daten und vertraulichen Informationen und den Diensten, Systemen, Geräten oder Medien, die diese Informationen enthalten, zu verhindern.

3.7 Setzen Sie Risikobewertungsprozesse und -verfahren ein, um regelmäßig Systeme zu bewerten, die zur Bereitstellung von Dienstleistungen oder Produkten für CWT verwendet werden. Der Anbieter wird solche Risiken so schnell wie vernünftigerweise möglich und entsprechend dem Risikoniveau für personenbezogene Daten und vertrauliche Informationen angesichts der zum Zeitpunkt der Identifizierung bekannten Bedrohungen beheben. Führen Sie einen Prozess durch, um das Melden von Risiken oder vermuteten Vorfällen an das Sicherheitsteam des Anbieters zu ermöglichen.

3.8 Soweit der Anbieter Dienstleistungen gemäß dem Vertrag in CWT-Einrichtungen erbringt oder Dienste, Systeme, Geräte oder Medien nutzt, die CWT gehören, von CWT betrieben oder verwaltet werden, muss der Anbieter alle autorisierten Parteien veranlassen, alle dem Anbieter zur Verfügung gestellten CWT-Richtlinien einzuhalten Anfrage, die für diesen Zugriff gelten. Der Anbieter muss CWT unverzüglich schriftlich benachrichtigen, wenn eine autorisierte Partei keinen Zugriff mehr auf die personenbezogenen Daten oder vertraulichen Informationen benötigt, damit der Anbieter Produkte oder Dienstleistungen für CWT bereitstellen kann , einschließlich, aber nicht beschränkt auf , wenn eine autorisierte Partei gekündigt wird oder anderweitig nicht mehr funktioniert Dienstleistungen im Rahmen der Vereinbarung.

3.9 Sie Aufzeichnungen über autorisierte Parteien und Lieferantenressourcen, die auf personenbezogene Daten und vertrauliche Informationen zugreifen, diese übertragen, pflegen, speichern oder verarbeiten.

3.10 Führen Sie vor der Einstellung umfassende Hintergrundprüfungen aller autorisierten Parteien durch, soweit dies gesetzlich zulässig ist . Die umfassende Hintergrundüberprüfung von Personen umfasst mindestens die bisherige Beschäftigungshistorie, das Vorstrafenregister, die Kredithistorie, Referenzprüfungen und alle zusätzlichen branchenüblichen Hintergrundüberprüfungsanforderungen der Person.

3.11 Ein oder mehrere qualifizierte Mitarbeiter haben, die für die Pflege seines Informationssicherheitsprogramms verantwortlich sind und mindestens einmal jährlich dem Vorstand des Anbieters oder einem gleichwertigen Leitungsgremium über sein Informationssicherheitsprogramm Bericht erstatten. Der Anbieter stellt sicher, dass sein Sicherheitspersonal über angemessene und notwendige Erfahrung und Schulung in Informationssicherheit verfügt, einschließlich der Aufrechterhaltung des Wissens über sich ändernde Bedrohungen und Gegenmaßnahmen. Auf Anfrage stellt der Anbieter CWT eine Kontaktstelle für alle Fragen im Zusammenhang mit der Informationssicherheit zur Verfügung.

3.12 Fordern Sie vertragliche Verpflichtungen zur Geheimhaltung oder Vertraulichkeit von autorisierten Parteien, bevor Sie ihnen Zugang zu personenbezogenen Daten und vertraulichen Informationen gewähren.

3.13 Stellen Sie sicher, dass alle autorisierten Parteien, die möglicherweise Arbeiten im Rahmen der Vereinbarung ausführen oder Zugriff auf personenbezogene Daten oder vertrauliche

Informationen haben, diese technischen und organisatorischen Sicherheitsmaßnahmen einhalten, die durch eine schriftliche Vereinbarung belegt werden, die nicht weniger restriktiv ist als diese Informationssicherheitsanforderungen .

4. Physische und Umgebungssicherheit

Der Anbieter muss mindestens :

4.1 Stellen Sie sicher, dass sich alle Systeme und anderen Ressourcen des Anbieters, die für die Verwendung durch mehrere Benutzer vorgesehen sind, in sicheren physischen Einrichtungen befinden, deren Zugriff auf autorisierte Personen beschränkt und beschränkt ist.

4.2 Überwachung und Aufzeichnung zu Prüfungszwecken, Zugang zu den physischen Einrichtungen, die Systeme und andere Ressourcen enthalten, die für die Verwendung durch mehrere Benutzer bestimmt sind und die im Zusammenhang mit der Erfüllung der Verpflichtungen des Anbieters aus dem Vertrag verwendet werden.

4.3 Fordern Sie alle autorisierten Parteien auf, sich an eine Richtlinie für saubere Schreibtische zu halten und die Bildschirme der Arbeitsplätze zu sperren, bevor Sie die Arbeitsbereiche verlassen.

4.4 Sammeln Sie alle Vermögenswerte des Unternehmens bei Beendigung des Arbeitsverhältnisses oder der Vertragsbeendigung.

4.5 Beschränken und überwachen Sie den physischen Zugang zu seinen Einrichtungen gemäß den folgenden Anforderungen:

a. Der Besucherzugang wird protokolliert und für drei (3) Monate aufbewahrt, einschließlich des Namens des Besuchers, des Unternehmens, das er/sie vertritt, und des Namens des Mitarbeiters, der den physischen Zugang autorisiert. Besucher müssen jederzeit von einem Mitarbeiter des Anbieters begleitet werden.
b. Der Zugriff ist auf geeignetes Personal beschränkt, basierend auf einer Need-to-know-Basis.
c. Alle Mitarbeiter müssen ein firmeneigenes Namensschild und alle Besucher oder Dritte einen firmeneigenen Gast-/Besucherausweis tragen.
d. Der Zugang wird sofort nach Kündigung des Personals des Anbieters oder Dritter widerrufen , und alle physischen Zugangsmechanismen wie Schlüssel, Zugangskarten usw. werden zurückgegeben oder deaktiviert.
e. Das Rechenzentrum oder der Computerraum ist verschlossen und der Zugang ist auf diejenigen beschränkt, die Zugang zur Erfüllung ihrer beruflichen Pflichten benötigen.
f. Verwenden Sie, wo gesetzlich zulässig, Videokameras, um den physischen Zugang zu sensiblen Bereichen zu überwachen, und überprüfen Sie diese Daten regelmäßig. Videomaterial muss mindestens drei (3) Monate lang aufbewahrt werden.
g. Geräte, die zum Speichern, Verarbeiten oder Übertragen personenbezogener Daten und vertraulicher Daten verwendet werden, müssen physisch gesichert werden,

einschließlich drahtloser Zugangspunkte, Gateways, Handheld-Geräte, Netzwerk-/Kommunikationshardware und Telekommunikationsleitungen.

4.6 Implementieren Sie Kontrollen, um das Risiko physischer Bedrohungen zu minimieren und sich davor zu schützen.

4.7 Pflegen Sie alle Hardware-Assets, die personenbezogene Daten und vertrauliche Informationen verarbeiten oder handhaben, gemäß den vom Hersteller empfohlenen Wartungsanforderungen.

4.8 Schränken Sie Konferenzräume und andere öffentlich zugängliche Netzwerke und Netzwerkbuchsen logisch und physisch vom internen Netzwerk des Anbieters ein und beschränken Sie sie nur auf authentifizierte Benutzer oder deaktivieren Sie sie standardmäßig.

4.9 Schützen Sie jedes Gerät, das Zahlungskartendaten über direkte physische Interaktion erfasst, vor Manipulation und Austausch, indem Sie die Geräteoberflächen regelmäßig untersuchen, um Manipulationen oder Austausch festzustellen; Personal schulen, damit es auf Manipulationsversuche oder den Austausch von Geräten achtet.

4.10 Kontrollieren und trennen Sie Zugangspunkte wie Liefer- und Ladebereiche und andere Punkte von allen Zentren, die auf personenbezogene und vertrauliche Informationen zugreifen, diese verwalten, speichern oder verarbeiten.

4.11 Stellen Sie sicher, dass die Rechenzentren der Anbieter über Heizungs-, Kühlungs-, Feuerunterdrückungs-, Wassererkennungs- und Hitze-/Raucherkennungsgeräte verfügen. Rechenzentren und Computerräume von Herstellern müssen frei von brennbaren Materialien (z . B. Kartons, Papier usw.) sein oder in Metallschränken gelagert werden.

5. <u>Zugangskontrolle</u>

Der Anbieter muss mindestens :

5.1 Ergreifen Sie alle angemessenen Schritte, um zu verhindern, dass andere Personen als autorisierte Parteien auf personenbezogene Daten und vertrauliche Informationen in irgendeiner Weise oder zu irgendeinem Zweck zugreifen, der nicht von CWT und der Vereinbarung autorisiert ist.

5.2 Trennen Sie die Informationen von CWT von den Daten anderer Kunden des Anbieters oder den eigenen Anwendungen und Informationen des Anbieters, indem Sie entweder physisch getrennte Server verwenden oder logische Zugriffskontrollen verwenden, wenn keine physische Trennung von Servern implementiert ist.

5.3 Identifizieren und fordern Sie die entsprechenden Eigentümer auf, den Zugriff auf Systeme, die für den Zugriff auf, die Verarbeitung, Verwaltung oder Speicherung von personenbezogenen Daten und vertraulichen Informationen verwendet werden , mindestens

vierteljährlich zu überprüfen und zu genehmigen, um den unbefugten Zugriff zu entfernen ; und Zugriffsgenehmigungen verwalten und nachverfolgen.

5.4 Den Zugriff auf Systeme, die personenbezogene Daten und vertrauliche Informationen verwalten, innerhalb von 24 Stunden nach Beendigung der Beziehung der autorisierten Partei mit dem Anbieter entfernen; und angemessene Verfahren aufrechterhalten, um den Zugriff auf solche Systeme innerhalb von drei Geschäftstagen zu entfernen, wenn er nicht mehr benötigt wird oder für die Erfüllung ihrer Pflichten relevant ist . Alle anderen Benutzer-IDs müssen nach 90 Kalendertagen Inaktivität deaktiviert oder entfernt werden.

5.5 Beschränken Sie den Zugriff des Systemadministrators (auch bekannt als Root, privilegierter oder Superuser) auf Betriebssysteme, die von mehreren Benutzern verwendet werden sollen, nur auf Personen, die einen solchen High-Level-Zugriff für die Ausführung ihrer Arbeit benötigen. Verwenden Sie Check-out-Systemadministrator-IDs mit individuellen Benutzeranmeldeinformationen und Aktivitätsprotokollen, um den Hochsicherheitszugriff zu verwalten und den High-Level-Zugriff auf eine stark begrenzte Anzahl von Benutzern zu reduzieren. Fordern Sie Anwendungs-, Datenbank-, Netzwerk- und Systemadministratoren auf, den Zugriff von Benutzern nur auf die Befehle, Daten, Systeme und anderen Ressourcen zu beschränken, die für die Ausführung autorisierter Funktionen erforderlich sind. Systemadministrationsrollen und Zugriffslisten müssen mindestens einmal jährlich überprüft werden.

5.6 Setzen Sie die Regel des geringsten Privilegs durch (dh beschränken Sie den Zugriff auf nur die Befehle, Informationen, Systeme und andere Ressourcen, die erforderlich sind, um autorisierte Funktionen gemäß der eigenen beruflichen Funktion auszuführen).

5.7 Fordern Sie eine starke Authentifizierung für alle administrativen Zugriffe außerhalb der Konsole , alle Remotezugriffe und alle administrativen Zugriffe auf Cloud-Umgebungen .

5.8 Verbieten und setzen Sie technische und organisatorische Sicherheitsmaßnahmen ein, um sicherzustellen, dass personenbezogene Daten nicht kopiert, verschoben oder auf lokalen Festplatten gespeichert oder personenbezogene Daten ausgeschnitten und eingefügt oder gedruckt werden können.

5.9 Aktivieren Sie die Verwendung von Fernzugriffsfunktionen nur bei Bedarf, überwachen Sie sie während der Verwendung und deaktivieren Sie sie sofort nach der Verwendung.

5.10 Fordern Sie eine starke Authentifizierung an, um eine Verbindung zu internen Ressourcen des Anbieters herzustellen, die personenbezogene und vertrauliche Informationen enthalten.

6. <u>Identifizierung und Authentifizierung</u>

Der Anbieter muss mindestens :

6.1 Weisen Sie einzelnen Benutzern eindeutige Benutzer-IDs zu und weisen Sie jedem einzelnen Konto Authentifizierungsmechanismen zu.

6.2 Verwenden Sie einen dokumentierten Benutzer-ID-Lebenszyklus-Managementprozess, einschließlich, aber nicht beschränkt auf Verfahren zur genehmigten Kontoerstellung, rechtzeitigen Kontoentfernung und Kontoänderung (z. B. Änderungen an Berechtigungen, Zugriffsspanne, Funktionen/Rollen) für den gesamten Zugriff auf personenbezogene Daten und Vertrauliche Informationen und in allen Umgebungen (z. B. Produktion, Test, Entwicklung usw.). Dieser Prozess muss mindestens vierteljährlich eine Überprüfung der Zugriffsrechte und der Kontogültigkeit umfassen.

6.3 Beschränken Sie den Zugriff auf personenbezogene Daten und vertrauliche Informationen auf diejenigen, die eine gültige Benutzer-ID und ein gültiges Passwort verwenden, und verlangen Sie, dass eindeutige Benutzer-IDs eine der folgenden Methoden verwenden: Passwort oder Passphrase, Zwei-Faktor-Authentifizierung oder einen biometrischen Wert.

6.4 Erfordern Sie Passwortkomplexität und erfüllen Sie die folgenden Anforderungen an den Passwortaufbau: mindestens zwölf (12) Zeichen lang für Systempasswörter und vier (4) Zeichen für Tablet- und Smartphone-Passcodes. Systemkennwörter müssen drei (3) der folgenden Zeichen enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern oder Sonderzeichen. Passwörter dürfen auch nicht mit der Benutzer-ID identisch sein, mit der sie verknüpft sind, ein Wörterbuchwort, fortlaufende oder sich wiederholende Zahlen enthalten und nicht eines der letzten 24 Passwörter sein. Verlangen Sie, dass das Kennwort in regelmäßigen Abständen abläuft und neunzig (90) Tage nicht überschreitet. Maskieren Sie alle Passwörter, wenn sie angezeigt werden.

6.5 Begrenzen Sie fehlgeschlagene Anmeldeversuche auf nicht mehr als fünf (5) fehlgeschlagene Anmeldeversuche innerhalb von 24 Stunden und sperren Sie das Benutzerkonto bei Erreichen dieses Limits dauerhaft. Der Zugriff auf das Benutzerkonto kann nachträglich durch einen manuellen Prozess, der eine Überprüfung der Identität des Benutzers erfordert, wieder aktiviert werden.

6.6 Überprüfen Sie die Identität des Benutzers und legen Sie Passwörter zur einmaligen Verwendung fest und setzen Sie Passwörter auf einen eindeutigen Wert für jeden Benutzer zurück. Systematisch zeitnaher Wechsel nach Erstgebrauch.

6.7 Verwenden Sie eine sichere Methode für die Übermittlung von Authentifizierungsnachweisen (z. B. Passwörtern) und Authentifizierungsmechanismen (z. B. Token oder Smartcards).

6.8 Beschränken Sie Passwörter für Dienstkonten und Proxys auf mindestens 20 Zeichen , einschließlich Großbuchstaben, Kleinbuchstaben und Ziffern sowie Sonderzeichen. Ändern Sie die Passwörter für Dienstkonten und Proxys mindestens jährlich und nach Beendigung des Arbeitsverhältnisses von Personen, die das Passwort kennen.

6.9 Beenden Sie interaktive Sitzungen oder aktivieren Sie einen sicheren, sperrenden Bildschirmschoner, der eine Authentifizierung erfordert, nach einem Zeitraum der Inaktivität von höchstens fünfzehn (15) Minuten.

6.10 Verwenden Sie eine Authentifizierungsmethode, die auf der Sensibilität von personenbezogenen und vertraulichen Informationen basiert. Wann immer Authentifizierungsdaten gespeichert werden, muss der Anbieter diese mit starker Verschlüsselung schützen.

6.11 Konfigurieren Sie Systeme so, dass sie nach einem maximalen Zeitraum der Inaktivität automatisch ablaufen : Server (15 Minuten), Workstation (15 Minuten), mobiles Gerät (4 Stunden), Dynamic Host Configuration Protocol (7 Tage), Virtual Private Network (24 Stunden).

7. Beschaffung, Entwicklung und Wartung von Informationssystemen

Der Anbieter muss mindestens :

7.1 Zeigen Sie ein Warnbanner auf Anmeldebildschirmen oder -seiten an, wie von CWT schriftlich für Produkte oder Dienstleistungen der Marke CWT oder für Produkte und Software, die für CWT entwickelt wurden, angegeben wurde.

7.2 Geben Sie alle CWT-eigenen oder von CWT bereitgestellten Zugangsgeräte so bald wie möglich zurück, in keinem Fall jedoch später als fünfzehn (15) Tage nach dem frühesten der folgenden:

a. Ablauf oder Kündigung der Vereinbarung;
b. Aufforderung von CWT zur Rückgabe dieses Eigentums; oder
c. das Datum, an dem der Anbieter solche Geräte nicht mehr benötigt.

7.3 Wenden Sie eine effektive Methodik für das Anwendungsmanagement an, die technische und organisatorische Sicherheitsmaßnahmen in den Softwareentwicklungsprozess einbezieht, und stellen Sie sicher, dass technische und organisatorische Sicherheitsmaßnahmen, wie sie in den Best Practices der Branche dargestellt werden, vom Anbieter rechtzeitig implementiert werden.

7.4 Befolgen Sie branchenübliche Entwicklungsverfahren, einschließlich der Trennung von Zugriff und Code zwischen Nicht-Produktions- und Produktionsumgebungen und der damit verbundenen Aufgabentrennung zwischen diesen Umgebungen.

7.5 Sicherstellen, dass interne Informationssicherheitskontrollen für die Softwareentwicklung regelmäßig bewertet werden und die Best Practices der Branche widerspiegeln, und diese Kontrollen zeitnah überarbeiten und implementieren.

7.6 Verwalten Sie die Sicherheit des Entwicklungsprozesses und stellen Sie sicher, dass sichere Codierungspraktiken implementiert und befolgt werden, einschließlich geeigneter kryptografischer Kontrollen, Schutz vor bösartigem Code und eines Peer-Review-Prozesses.

7.7 Führen Sie Penetrationstests für funktional vollständige Anwendungen durch, bevor Sie sie in die Produktion geben und danach mindestens einmal jährlich und nach allen wesentlichen Änderungen am Quellcode oder an der Konfiguration, die mit OWASP, CERT, SANS Top 25 und PCI-DSS übereinstimmen. Beheben Sie alle ausnutzbaren Schwachstellen vor der Bereitstellung in der Produktionsumgebung.

7.8 Verwenden Sie anonymisierte oder verschleierte Daten in Nicht-Produktionsumgebungen. Verwenden Sie niemals Klartext-Produktionsdaten in einer Nicht-Produktionsumgebung und verwenden Sie niemals personenbezogene Daten aus irgendeinem Grund in Nicht-Produktionsumgebungen. Stellen Sie sicher, dass alle Testdaten und Konten vor der Produktionsfreigabe entfernt werden.

7.9 Überprüfen Sie von CWT genehmigten Open- oder Free-Source-Code, Software, Anwendungen oder Services auf Fehler, Bugs, Sicherheitsprobleme oder Nichteinhaltung von Open- oder Free-Source-Lizenzbedingungen. Der Anbieter muss CWT im Voraus über die Verwendung von offenem oder kostenlosem Quellcode informieren und CWT den Namen, die Version und die URL des offenen oder kostenlosen Quellcodes mitteilen, falls die Verwendung durch CWT genehmigt wurde. Der Anbieter erklärt und garantiert, dass (a) jeder offene oder kostenlose Quellcode, den er in seinen Produkten oder Dienstleistungen verwendet, unter „permissiven“ offenen oder kostenlosen Quellcodelizenzen und nicht unter restriktiven, reziproken, erblichen oder Copyleft-Lizenzen lizenziert ist; (b) Der Anbieter hat das Recht, offenen oder freien Quellcode frei zu ändern, anzupassen und offenen oder freien Quellcode zu kombinieren oder offenen oder freien Quellcode mit proprietärem Code zu enthalten, ohne Beschränkungen für solche Änderungen, Anpassungen oder Kombinationen oder proprietären Code, der enthält Open- oder Free -Source-Code und wie diese weiter lizenziert werden können (zusammen „ **abgeleitete Werke** “) und (c) solche abgeleiteten Werke unterliegen keiner Open- oder Free-Source-Lizenz, die eine Lizenzierung des abgeleiteten Werks oder dessen kostenlose Bereitstellung erfordert an Dritte unter den Open- oder Free-Source-Lizenzbedingungen.

7.10 Teilen Sie keinen im Rahmen der Vereinbarung erstellten Code, unabhängig vom Entwicklungsstadium, in einer gemeinsam genutzten oder nicht privaten Umgebung, wie z. B. einem Open-Access-Code-Repository, unabhängig vom Passwortschutz.

8. Software- und Datenintegrität

Der Anbieter muss mindestens :

8.1 Lassen Sie in Umgebungen, in denen Antivirensoftware im Handel erhältlich ist, aktuelle Antivirensoftware installieren und ausführen, um nach Viren und anderer Malware zu suchen und diese umgehend von allen Systemen oder Geräten zu entfernen oder zu isolieren.

8.2 Trennen Sie Nichtproduktionsinformationen und -ressourcen von Produktionsinformationen und -ressourcen.

8.3 Stellen Sie sicher, dass Teams einen dokumentierten Änderungskontrollprozess für alle Systemänderungen verwenden, einschließlich Back-out-Verfahren für alle Produktionsumgebungen und Notfalländerungsprozesse. Schließen Sie Tests, Dokumentation und Genehmigungen für alle Systemänderungen ein und verlangen Sie die Genehmigung des Managements für wesentliche Änderungen in solchen Prozessen.

8.4 Erstellen und pflegen Sie eine PCI-Zone, wenn der Anbieter Karteninhaberdaten verarbeitet oder speichert.

8.5 Aktivieren und pflegen Sie für Anwendungen, die eine Datenbank verwenden, die Änderungen an personenbezogenen und vertraulichen Informationen zulässt , Überwachungsprotokollierungsfunktionen für Datenbanktransaktionen, die Überwachungsprotokolle für Datenbanktransaktionen mindestens ein (1) Jahr lang aufbewahren und drei Monate sofort zur Analyse zur Verfügung stehen.

8.6 Überprüfen Sie die Software, um Sicherheitslücken während der Erstimplementierung und bei wesentlichen Änderungen und Aktualisierungen zu finden und zu beheben.

8.7 Durchführung von Qualitätssicherungstests für die Sicherheitskomponenten (z. B. Testen von Identifizierungs-, Authentifizierungs- und Autorisierungsfunktionen) sowie alle anderen Aktivitäten zur Validierung der Sicherheitsarchitektur während der Erstimplementierung und bei allen wesentlichen Änderungen und Aktualisierungen.

9. Systemsicherheit

Der Anbieter muss mindestens :

9.1 Erstellen und aktualisieren Sie regelmäßig die neuesten Versionen von Datenfluss- und Systemdiagrammen, die für den Zugriff auf, die Verarbeitung, Verwaltung oder Speicherung von personenbezogenen und vertraulichen Informationen verwendet werden.

9.2 Überwachen Sie aktiv Branchenressourcen (z. B. , www.cert.org und relevante Mailinglisten und Websites von Softwareanbietern) auf rechtzeitige Benachrichtigung über alle anwendbaren Sicherheitswarnungen, die sich auf die Systeme des Anbieters und andere Informationsressourcen beziehen.

9.3 Verwalten Sie kryptografische Schlüssel effektiv, indem Sie den Zugriff auf Schlüssel auf die geringstmögliche Anzahl von Verwaltern reduzieren, geheime und private kryptografische Schlüssel speichern, indem Sie mit einem Schlüssel verschlüsseln, der mindestens so stark ist wie der Datenverschlüsselungsschlüssel, und getrennt vom Datenverschlüsselungsschlüssel in einem sicheren Bereich speichern kryptografisches Gerät an möglichst wenigen Standorten. Ändern Sie bei der Installation und mindestens alle zwei Jahre die standardmäßigen kryptografischen Schlüssel und entsorgen Sie alte Schlüssel sicher.

9.4 Scannen Sie nach außen gerichtete und interne Systeme und andere Informationsressourcen, einschließlich, aber nicht beschränkt auf Netzwerke, Server, Anwendungen und Datenbanken, mit anwendbarer branchenüblicher Software zum Scannen von Sicherheitslücken, um Sicherheitslücken aufzudecken, und stellen Sie sicher, dass solche Systeme und andere Ressourcen ordnungsgemäß funktionieren gehärtet, und identifizieren Sie alle nicht autorisierten drahtlosen Netzwerke mindestens vierteljährlich und vor der Freigabe für Anwendungen und für wesentliche Änderungen und Upgrades innerhalb von Zeitrahmen, die sich aus Risikoanalysen ergeben, die auf angemessenen und allgemein anerkannten IT-Richtlinien und -Standards basieren.

9.5 Stellen Sie sicher, dass alle Systeme und anderen Ressourcen des Anbieters gehärtet sind und bleiben, einschließlich, aber nicht beschränkt auf, das Entfernen oder Deaktivieren nicht verwendeter Netzwerk- und anderer Dienste und Produkte (z. B. Finger, rlogin, FTP und Simple Transmission Control Protocol/Internet Protocol (TCP/ IP)-Dienste und -Produkte) und die Installation einer System-Firewall, TCP-Wrapper (Transmission Control Protocol) oder ähnlicher Technologien.

9.6 Stellen Sie ein oder mehrere Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) oder Intrusion Detection and Prevention Systems (IDP) in einem aktiven Betriebsmodus bereit, der den gesamten eingehenden und ausgehenden Datenverkehr und andere Ressourcen in Verbindung mit der Vereinbarung überwacht Umgebungen, in denen eine solche Technologie im Handel erhältlich und soweit praktikabel ist.

9.7 Pflegen Sie einen Risikobewertungsprozess für die Ergebnisse der Schwachstellenbewertung, der an den Best Practices der Branche ausgerichtet ist, um Sicherheitslücken in allen Systemen oder anderen Ressourcen zu beheben, einschließlich, aber nicht beschränkt auf solche, die durch Branchenveröffentlichungen, Schwachstellen-Scans, Virenscans und die Überprüfung von Sicherheitsprotokollen entdeckt wurden und im Hinblick auf die Wahrscheinlichkeit, dass eine solche Schwachstelle ausgenutzt werden kann oder gerade ausgenutzt wird, unverzüglich geeignete Sicherheitspatches anzuwenden. Kritische Schwachstellenbewertungsergebnisse und Patches müssen sofort nach Verfügbarkeit und in keinem Fall länger als 7 Tage nach der Veröffentlichung behoben werden. Hohe Schwachstellenbewertungsergebnisse und Patches müssen innerhalb von 30 Tagen nach der Veröffentlichung behoben werden. Mittlere Schwachstellenbewertungsergebnisse und Patches müssen innerhalb von 90 Kalendertagen behoben werden. Niedrige Schwachstellenbewertungsergebnisse und Patches müssen innerhalb von 120 Kalendertagen behoben werden.

9.8 Führen Sie Netzwerk- und Segmentierungs-Penetrationstests intern und extern mindestens einmal jährlich und nach jeder wesentlichen Infrastruktur- oder Anwendungsaktualisierung oder -änderung durch.

9.9 Entfernen oder deaktivieren Sie nicht autorisierte Software, die auf den Systemen des Anbieters entdeckt wurde, und wenden Sie branchenübliche Malware-Kontrollen an, einschließlich der Installation, regelmäßigen Aktualisierung und routinemäßigen Verwendung

von Anti-Malware-Softwareprodukten auf allen Diensten, Systemen und Geräten, die für den Zugriff auf personenbezogene Daten und CWT verwendet werden können Vertrauliche Informationen. Verwenden Sie nach Möglichkeit zuverlässige und branchenweit bewährte Antivirensoftware und stellen Sie sicher, dass diese Virendefinitionen immer auf dem neuesten Stand sind.

9.10 Halten Sie die Software auf allen Diensten, Systemen und Geräten, die für den Zugriff auf personenbezogene Daten und vertrauliche Informationen von CWT verwendet werden können, auf dem neuesten Stand, einschließlich der angemessenen Wartung des/der Betriebssystem(e) und der erfolgreichen Installation einigermaßen aktueller Sicherheitspatches.

9.11 Weisen Sie bestimmten Personen Verantwortlichkeiten für die Sicherheitsadministration für die Konfiguration von Host-Betriebssystemen zu.

9.12 Ändern Sie alle Standardkontonamen und/oder Standardpasswörter.

10. Überwachung

Der Anbieter muss mindestens :

10.1 Bewahren Sie Protokolldaten für personenbezogene Daten und vertrauliche Informationen für mindestens 12 Monate ab dem Datum der Erstellung der Protokolldaten auf und stellen Sie das Protokoll und diese Daten CWT innerhalb eines angemessenen Zeitraums und auf Anfrage zur Verfügung, sofern dies nicht an anderer Stelle in der Vereinbarung festgelegt ist. Protokolle müssen darauf ausgelegt sein, Vorfälle zu erkennen und darauf zu reagieren, und beinhalten, sind aber nicht beschränkt auf:

a. Alle individuellen Benutzerzugriffe auf personenbezogene Daten und vertrauliche Informationen
b. Alle Aktionen, die von Benutzern mit Administrator- oder Root-Rechten ausgeführt werden
c. Aller Benutzerzugriff auf Audit-Trails
d. Ungültige logische Zugriffsversuche
e. Verwendung und Änderung von Identifizierungs- und Authentifizierungsmechanismen

10.2 Zeichnen Sie die primären Systemaktivitäten des Drittanbieters des Anbieters für Systeme auf, die personenbezogene Daten und vertrauliche Informationen enthalten, und verfügen Sie über ein formelles Drittanbieter-Sicherheitsprogramm, um sicherzustellen, dass die Drittanbieter oder Subunternehmer des Anbieters über angemessene Sicherheitskontrollen und Zertifizierungen verfügen. Lassen Sie eine Cloud-Sicherheitsbewertung durchführen, wenn CWT Daten befinden sich in einer Cloud-Umgebung.

10.3 Beschränken Sie den Zugriff auf Sicherheitsprotokolle auf autorisierte Personen und schützen Sie Sicherheitsprotokolle vor unbefugter Änderung.

10.4 Implementieren Sie einen Änderungserkennungsmechanismus (z . B. Überwachung der Dateiintegrität), um das Personal vor unbefugter Änderung kritischer Systemdateien, Konfigurationsdateien oder Inhaltsdateien zu warnen; Konfigurieren Sie die Software so, dass sie wöchentlich wichtige Dateivergleiche durchführt.

10.5 Überprüfen Sie mindestens wöchentlich alle Sicherheits- und sicherheitsbezogenen Prüfprotokolle auf Systemen, die personenbezogene Daten und vertrauliche Informationen enthalten, auf Anomalien und dokumentieren und beheben Sie alle protokollierten Sicherheitsprobleme zeitnah.

10.6 Überprüfen Sie täglich alle Sicherheitsereignisse, Protokolle von Systemkomponenten, die Karteninhaberdaten speichern, verarbeiten oder übertragen, Protokolle von kritischen Systemkomponenten und Protokolle von Servern und Systemkomponenten, die Sicherheitsfunktionen ausführen.

11. Sicherheitsgateways

Der Anbieter muss mindestens :

11.1 Fordern Sie eine starke Authentifizierung für den Administrator- und/oder Verwaltungszugriff auf Sicherheits-Gateways, einschließlich, aber nicht beschränkt auf Zugriffe zum Zwecke der Überprüfung von Protokolldateien.

11.2 Haben und verwenden Sie dokumentierte Kontrollen, Richtlinien, Prozesse und Verfahren, um sicherzustellen, dass unbefugte Benutzer keinen Administrator- und/oder Verwaltungszugriff auf Security Gateways haben und dass die Benutzerautorisierungsebenen zum Verwalten und Verwalten von Security Gateways angemessen sind.

11.3 Haben Sie strenge Kontrollen rund um die E-Mail-Sicherheit, wie z. B. die Konfiguration von DKIM- und SPF-Authentifizierungsprotokollen, die dabei helfen, zu validieren, dass eine E-Mail-Nachricht von einer vertrauenswürdigen und validierten Quelle stammt. Implementierung von DMARC auf empfangenden E-Mail-Servern.

11.4 Stellen Sie mindestens einmal alle sechs (6) Monate sicher, dass die Security Gateway-Konfigurationen gehärtet sind, indem Sie eine Stichprobe von Security Gateways auswählen und überprüfen, ob jeder Standardregelsatz und Satz von Konfigurationsparametern Folgendes gewährleistet:

a. Internet Protocol (IP)-Quellrouting ist deaktiviert,
b. Die Loopback-Adresse darf nicht in das interne Netzwerk gelangen,
c. Anti-Spoofing-Filter sind implementiert,
d. Broadcast-Pakete dürfen nicht in das Netzwerk gelangen,
e. ICMP-Umleitungen (Internet Control Message Protocol) sind deaktiviert,
f. Alle Regelsätze enden mit einer „DENY ALL“-Anweisung und
g. Jede Regel lässt sich auf eine bestimmte Geschäftsanforderung zurückverfolgen.

11.5 Stellen Sie sicher, dass Überwachungstools verwendet werden, um zu validieren, dass alle Aspekte von Security Gateways (z. B. Hardware, Firmware und Software) kontinuierlich betriebsbereit sind.

Stellen Sie sicher, dass alle Sicherheits-Gateways so konfiguriert und implementiert sind, dass alle nicht betriebsbereiten Sicherheits-Gateways jeglichen Zugriff verweigern.

11.6 Eingehende Pakete aus dem nicht vertrauenswürdigen externen Netzwerk müssen innerhalb der entmilitarisierten Zone („ **DMZ** “) enden und dürfen nicht direkt zum vertrauenswürdigen internen Netzwerk fließen. Alle eingehenden Pakete, die zum vertrauenswürdigen internen Netzwerk fließen, dürfen nur aus der DMZ stammen. Die DMZ muss vom nicht vertrauenswürdigen externen Netzwerk durch die Verwendung eines Sicherheits-Gateways und vom vertrauenswürdigen internen Netzwerk durch eine der folgenden Methoden getrennt werden:

a. ein anderes Sicherheits-Gateway, oder
b. dasselbe Sicherheitsgateway, das verwendet wird, um die DMZ vom nicht vertrauenswürdigen externen Netzwerk zu trennen. In diesem Fall muss das Sicherheitsgateway sicherstellen, dass Pakete, die vom nicht vertrauenswürdigen externen Netzwerk empfangen werden, entweder sofort gelöscht oder, wenn sie nicht gelöscht werden, nur an die DMZ ohne weitere Verarbeitung weitergeleitet werden solche eingehenden Pakete werden anders durchgeführt, als die Pakete möglicherweise in ein Protokoll zu schreiben.

Folgendes darf sich nur innerhalb des vertrauenswürdigen internen Netzwerks befinden:

a. Alle personenbezogenen Daten und vertraulichen Informationen von CWT, die ohne starke Verschlüsselung gespeichert werden,
b. Die offizielle Kopie der Informationen
c. Datenbankserver,
d. Alle exportierten Protokolle und
e. Alle Umgebungen, die für Entwicklung, Test, Sandbox, Produktion und andere derartige Umgebungen verwendet werden; und alle Quellcodeversionen.

11.7 Authentifizierungsdaten, die nicht durch starke Verschlüsselung geschützt sind, dürfen sich nicht innerhalb der DMZ befinden.

12. <u>Netzwerksicherheit</u>

Der Anbieter muss mindestens :

12.1 Stellen Sie CWT auf Anfrage ein logisches Netzwerkdiagramm zur Verfügung, das Systeme und Verbindungen zu anderen Ressourcen dokumentiert, darunter Router, Switches, Firewalls, IDS-Systeme, Netzwerktopologie, externe Verbindungspunkte, Gateways, drahtlose Netzwerke und alle anderen Geräte, die CWT unterstützen sollen.

12.2 Pflegen Sie einen formalen Prozess zum Genehmigen, Testen und Dokumentieren aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration. Konfigurieren Sie Firewalls so, dass sie verdächtige Pakete ablehnen und protokollieren, und schränken Sie sie so ein, dass nur angemessener und autorisierter Datenverkehr zugelassen wird, während der gesamte andere Datenverkehr durch die Firewall verweigert wird. Überprüfen Sie die Firewall-Regeln alle sechs Monate.

12.3 Installieren Sie eine Firewall an jeder Internetverbindung und zwischen jeder DMZ und der internen Netzwerkzone. Jedes System, das personenbezogene Daten speichert, muss sich in der internen Netzwerkzone befinden, getrennt von der DMZ und anderen nicht vertrauenswürdigen Netzwerken.

12.4 Überwachen Sie die Firewall am Perimeter und intern, um den Fluss des Netzwerkverkehrs, der die Grenze oder Grenze erreicht oder verlässt, nach Bedarf zu kontrollieren und zu schützen.

12.5 Installieren Sie Bedrohungserkennungstechnologien wie Network Detection and Response (NDR), Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR), die eine umfassende Lösung zur Erkennung und Reaktion auf verschiedene Cyberangriffe oder Ransomware-Angriffe bieten.

12.6 Führen Sie einen dokumentierten Prozess und Kontrollen ein, um unbefugte Zugriffsversuche auf personenbezogene Daten und vertrauliche Informationen von CWT zu erkennen und zu behandeln.

12.7 Schützen Sie bei der Bereitstellung von internetbasierten Diensten und Produkten für CWT personenbezogene Daten und vertrauliche Informationen durch die Implementierung einer Netzwerk-DMZ. Webserver, die Dienste für CWT bereitstellen, befinden sich in der DMZ. Alle Systeme oder Informationsressourcen, die personenbezogene Daten und vertrauliche Informationen speichern (wie Anwendungs- und Datenbankserver), müssen sich in einem vertrauenswürdigen internen Netzwerk befinden. Der Anbieter verwendet DMZ für Internetdienste und -produkte .

12.8 Beschränken Sie nicht autorisierten ausgehenden Datenverkehr von Anwendungen, die personenbezogene Daten und vertrauliche Informationen verarbeiten, speichern oder an IP-Adressen innerhalb der DMZ und des Internets übertragen.

12.9 Bei der Verwendung von Hochfrequenz-(RF)-basierten drahtlosen Netzwerktechnologien zur Erbringung oder Unterstützung von Dienstleistungen und Produkten für CWT muss der Anbieter sicherstellen, dass alle übertragenen personenbezogenen Daten und vertraulichen Informationen durch die Verwendung geeigneter Verschlüsselungstechnologien geschützt sind, die ausreichen, um die Vertraulichkeit personenbezogener Daten zu wahren und vertrauliche Informationen; vorausgesetzt jedoch, dass bei einer solchen Verschlüsselung auf jeden Fall nicht weniger als Schlüssellängen von 256 Bit für die symmetrische Verschlüsselung und 2048 Bit für die asymmetrische Verschlüsselung verwendet werden. Scannen, identifizieren und deaktivieren Sie regelmäßig nicht autorisierte drahtlose Zugriffspunkte.

12.10 Cloud-Sicherheit – Wenn sich die Daten von CWT in der Cloud befinden oder der Anbieter die Cloud-Umgebung eines Drittanbieters verwendet, einschließlich, aber nicht beschränkt auf Infrastructure as a Service (IaaS), Software as a Service (SaaS) und Platform as a Service (PaaS), muss der Anbieter dies tun Implementieren oder bewerten Sie Cloud Security Posture Management, um Bedrohungen, Fehlkonfigurationen, Missbrauch und Compliance-Verstöße in öffentlichen Clouds zu erkennen und automatisch zu beheben.

13. Konnektivitätsanforderungen

13.1 Für den Fall, dass der Anbieter im Zusammenhang mit der Vereinbarung eine Verbindung zu personenbezogenen Daten und vertraulichen Informationsressourcen von CWT hat oder bereitgestellt wird, muss der Anbieter zusätzlich zu dem Vorstehenden, wenn eine Verbindung zur Umgebung von CWT besteht oder bereitgestellt wird, unter a Minimum:

a. Verwenden Sie nur die gegenseitig vereinbarten Einrichtungen und Verbindungsmethoden, um die Umgebung von CWT mit den Ressourcen des Anbieters zu verbinden.
b. NIEMALS ohne die vorherige schriftliche Zustimmung von CWT eine Verbindung zur Umgebung von CWT herstellen.
c. Gewähren Sie CWT während der normalen Geschäftszeiten Zugang zu den entsprechenden Einrichtungen des Anbieters für die Wartung und den Support aller Geräte (z. B. Router), die von CWT im Rahmen der Vereinbarung für die Konnektivität mit Ressourcen für personenbezogene und vertrauliche Informationen bereitgestellt werden.
d. Verwenden Sie alle von CWT im Rahmen des Vertrags bereitgestellten Geräte für die Konnektivität mit der CWT-Umgebung nur für die Bereitstellung der Dienste und Produkte oder Funktionen, die ausdrücklich im Vertrag autorisiert sind.
e. Wenn die vereinbarte Konnektivitätsmethode erfordert, dass der Anbieter ein Sicherheits-Gateway implementiert, führen Sie Protokolle aller Sitzungen, die dieses Sicherheits-Gateway verwenden. Diese Sitzungsprotokolle müssen ausreichend detaillierte Informationen enthalten, um den Endbenutzer oder die Anwendung, die Ursprungs-IP-Adresse, die Ziel-IP-Adresse, die verwendeten Ports/Dienstprotokolle und die Zugriffsdauer zu identifizieren. Diese Sitzungsprotokolle müssen mindestens sechs (6) Monate nach Erstellung der Sitzung aufbewahrt werden.
f. Erlauben Sie CWT, Informationen über den Zugriff, einschließlich des Zugriffs des Anbieters, auf die Umgebung von CWT zu sammeln. Diese Informationen können von CWT gesammelt, gespeichert und analysiert werden, um potenzielle Sicherheitsrisiken ohne weitere Ankündigung zu identifizieren. Diese Informationen können Protokolldateien, Statistiken, Netzwerkadressen und die tatsächlichen Daten oder Bildschirme enthalten, auf die zugegriffen oder die übertragen wurden.
g. Unterbrechen oder beenden Sie unverzüglich jede Verbindung mit der Umgebung von CWT, wenn der Anbieter davon ausgeht, dass eine Sicherheitsverletzung oder ein unbefugter Zugriff vorliegt, oder auf Anweisung von CWT, wenn CWT nach eigenem Ermessen der Ansicht ist, dass eine Sicherheitsverletzung oder ein unbefugter Zugriff auf

oder ein Missbrauch von CWT-Dateneinrichtungen vorliegt oder jegliche Informationen, Systeme oder andere Ressourcen von CWT.

14. Mobile und tragbare Geräte

Der Anbieter muss mindestens :

14.1 Speichern Sie keine personenbezogenen Daten und vertraulichen Informationen auf mobilen und tragbaren Geräten, es sei denn, sie sind vollständig mit starker Verschlüsselung verschlüsselt.

14.2 Verwenden Sie eine starke Verschlüsselung, um personenbezogene und vertrauliche Informationen zu schützen, die von netzwerkfähigen mobilen und tragbaren Geräten übertragen, verwendet oder aus der Ferne abgerufen werden.

a. Bei der Verwendung netzwerkfähiger mobiler und tragbarer Geräte , die keine Laptops sind, um auf personenbezogene Daten und vertrauliche Informationen zuzugreifen und/oder diese zu speichern, müssen diese Geräte in der Lage sein, alle gespeicherten Kopien von personenbezogenen Daten und vertraulichen Informationen zu löschen, wenn sie über das Netzwerk eine ordnungsgemäß authentifizierte Person erhalten Befehl. (Hinweis: Eine solche Funktion wird oft als „Remote Wipe“-Funktion bezeichnet.)
b. Haben Sie dokumentierte Richtlinien, Verfahren und Standards eingerichtet, um sicherzustellen, dass die autorisierte Partei , die die physische Kontrolle über ein netzwerkfähiges mobiles und tragbares Gerät haben sollte, das kein Laptop ist und das personenbezogene und vertrauliche Informationen speichert, unverzüglich die Löschung aller einleitet Persönliche und vertrauliche Informationen, wenn das Gerät verloren geht oder gestohlen wird.
c. Verfügen Sie über dokumentierte Richtlinien, Verfahren und Standards, um sicherzustellen, dass mobile und tragbare Geräte, die keine Laptops sind und nicht netzwerkfähig sind, automatisch alle gespeicherten Kopien von personenbezogenen Daten und vertraulichen Daten nach aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen löschen.

14.3 Über dokumentierte Richtlinien, Verfahren und Standards verfügen, die sicherstellen, dass alle mobilen und tragbaren Geräte, die zum Zugreifen auf und/oder Speichern von personenbezogenen und vertraulichen Informationen verwendet werden:

a. sich im physischen Besitz autorisierter Parteien befinden ;
b. physisch gesichert sind, wenn sie sich nicht im physischen Besitz autorisierter Parteien befinden ; oder
c. Lassen Sie ihre Datenspeicher unverzüglich und sicher löschen, wenn sie sich nicht im physischen Besitz einer autorisierten Partei befinden oder physisch gesichert sind, oder nach 10 erfolglosen Zugriffsversuchen.

14.4 Vor der Gewährung des Zugriffs auf personenbezogene Daten und vertrauliche Informationen, die auf oder durch die Verwendung mobiler und tragbarer Geräte gespeichert sind, muss der Anbieter einen Prozess haben und anwenden, um sicherzustellen, dass:

a. Der Benutzer ist eine autorisierte Partei , die für diesen Zugriff autorisiert ist; und
b. Die Identität des Benutzers wurde authentifiziert.

14.5 Implementieren Sie eine Richtlinie, die die Verwendung von mobilen und tragbaren Geräten verbietet, die nicht vom Anbieter oder CWT verwaltet und/oder verwaltet werden, um auf personenbezogene Daten und vertrauliche Informationen zuzugreifen und/oder diese zu speichern.

14.6 Überprüfen Sie mindestens einmal jährlich die Nutzung und Kontrollen aller vom Anbieter verwalteten oder verwalteten mobilen und tragbaren Geräte, um sicherzustellen, dass die mobilen und tragbaren Geräte die anwendbaren technischen und organisatorischen Sicherheitsmaßnahmen erfüllen können.

15. Transportsicherheit

Der Anbieter muss mindestens :

15.1 Verwenden Sie starke Verschlüsselung für die Übertragung von personenbezogenen und vertraulichen Informationen außerhalb von CWT- oder anbietergesteuerten Netzwerken oder bei der Übertragung von personenbezogenen und vertraulichen Informationen über ein nicht vertrauenswürdiges Netzwerk.

15.2 Transportieren Sie Aufzeichnungen mit personenbezogenen und vertraulichen Informationen in Papierform, Mikrofiche oder elektronischen Medien, die physisch übertragen werden sollen, per gesichertem Kurier oder einer anderen Liefermethode, die nachverfolgt werden kann, sicher verpackt und gemäß den Herstellerspezifikationen. Alle personenbezogenen und vertraulichen Informationen müssen in verschlossenen Behältern transportiert werden.

16. Sicherheit im Ruhezustand

Der Anbieter muss mindestens :

16.1 Verwenden Sie eine starke Verschlüsselung, um persönliche und vertrauliche Informationen bei der Speicherung zu schützen.

16.2 Speichern Sie keine personenbezogenen oder vertraulichen Informationen elektronisch außerhalb der Netzwerkumgebung des Anbieters (oder des eigenen sicheren Computernetzwerks von CWT), es sei denn, das Speichergerät (z. B. Sicherungsband, Laptop, Speicherstick, Computerfestplatte usw.) ist durch starke Verschlüsselung geschützt.

16.3 Speichern Sie keine personenbezogenen oder vertraulichen Informationen auf Wechselmedien (z. B. USB-Flash-Laufwerke, USB-Sticks, Speichersticks, Bänder, CDs oder

externe Festplatten), außer: zu Backup-, Geschäftskontinuitäts-, Notfallwiederherstellungs- und Datenaustauschzwecken, soweit zulässig und vertraglich zwischen dem Anbieter und CWT erforderlich. Wenn Wechselmedien verwendet werden, um personenbezogene oder vertrauliche Informationen gemäß den in diesem Unterabschnitt genannten Ausnahmen zu speichern, müssen die Informationen mit starker Verschlüsselung geschützt werden. Autorun muss für Wechselmedien und Speichergeräte deaktiviert werden .

16.4 Bewahren und sichern Sie Aufzeichnungen mit personenbezogenen oder vertraulichen Informationen in Papierform oder Mikrofiche in Bereichen, zu denen der Zugriff auf autorisiertes Personal beschränkt ist.

16.5 Sofern von CWT nicht anders schriftlich angewiesen, stellen Sie beim Sammeln, Generieren oder Erstellen von personenbezogenen Daten oder vertraulichen Informationen in Papierform und auf Sicherungsmedien für, durch oder im Auftrag von CWT oder unter der Marke CWT sicher, dass es sich bei diesen Daten um personenbezogene Daten oder vertrauliche Informationen handelt und, wann immer möglich, solche Informationen von CWT als „vertraulich“ kennzeichnen. Der Anbieter erkennt an, dass personenbezogene Daten und vertrauliche Informationen Eigentum von CWT sind und bleiben – unabhängig von der Kennzeichnung oder deren Fehlen.

17. Rückgabe, Aufbewahrung, Vernichtung und Entsorgung

Der Anbieter muss mindestens :

17.1 Ohne zusätzliche Kosten für CWT stellen Sie CWT auf Anfrage von CWT oder bei Beendigung der Vereinbarung Kopien aller personenbezogenen Daten und vertraulichen Informationen innerhalb von dreißig (30) Kalendertagen nach einer solchen Anfrage oder Beendigung der Vereinbarung zur Verfügung . Der Anbieter muss alle vertraulichen Informationen und personenbezogenen Daten von CWT, einschließlich elektronischer , fester und gesicherter Sicherungskopien , wie in der Vereinbarung vorgesehen oder, falls nicht in der Vereinbarung vorgesehen, innerhalb von neunzig (90) Tage nach dem frühesten von: (a) Ablauf oder Kündigung des Vertrags, (b) CWTs Aufforderung zur Rückgabe personenbezogener Daten und vertraulicher Informationen oder (c) dem Datum, an dem der Anbieter keine personenbezogenen Daten und vertraulichen Informationen mehr benötigt, um Dienstleistungen zu erbringen und Produkte im Rahmen der Vereinbarung.

17.2 Für den Fall, dass CWT die Vernichtung als Alternative zur Rückgabe personenbezogener Daten und vertraulicher Informationen genehmigt, bestätigen Sie schriftlich durch einen leitenden Angestellten des Anbieters, dass die Vernichtung personenbezogene Daten und vertrauliche Informationen unwiederbringlich und unwiederbringlich macht. Der Anbieter muss alle Kopien von personenbezogenen Daten und vertraulichen Informationen an allen Orten und in allen Systemen, an denen personenbezogene Daten und vertrauliche Informationen gespeichert sind, einschließlich, aber nicht beschränkt auf zuvor genehmigte autorisierte Parteien , vollständig vernichten . Solche Informationen müssen gemäß einem branchenüblichen Verfahren zur vollständigen Vernichtung wie DOD 5220.22M oder NIST-Sonderveröffentlichung 800-88 oder unter Verwendung eines vom Hersteller empfohlenen

Entmagnetisierungsprodukts für das betroffene System vernichtet werden. Vor einer solchen Vernichtung muss der Anbieter alle anwendbaren technischen und organisatorischen Sicherheitsmaßnahmen aufrechterhalten, um die Sicherheit, den Datenschutz und die Vertraulichkeit von personenbezogenen und vertraulichen Informationen zu schützen.

17.3 Entsorgen Sie persönliche Informationen und vertrauliche Informationen von CWT auf eine Weise, die sicherstellt, dass die Informationen nicht in ein verwendbares Format rekonstruiert werden können. Papiere, Dias, Mikrofilme, Mikrofiche und Fotografien müssen quervernichtet oder verbrannt werden. Materialien, die personenbezogene Daten und vertrauliche Informationen von CWT enthalten, die auf die Vernichtung warten, müssen in gesicherten Behältern aufbewahrt und von einem sicheren Dritten transportiert werden.

18. Reaktion auf Vorfälle und Benachrichtigung

Der Anbieter muss mindestens :

18.1 Einen Incident-Management-Prozess und damit verbundene Verfahren haben und anwenden und einen solchen Incident-Management-Prozess und Verfahren mit spezialisierten Ressourcen besetzen. Benachrichtigen Sie CWT unverzüglich und auf keinen Fall länger als vierundzwanzig (24) Stunden unter iRespond@mycwt.com, wenn es einen vermuteten oder bestätigten Angriff auf, Eindringen, unbefugten Zugriff auf, Verlust oder einen anderen Vorfall in Bezug auf die Informationen von CWT gibt , Systeme oder andere Ressourcen.

18.2 Nachdem Sie CWT benachrichtigt haben, stellen Sie CWT regelmäßige Statusaktualisierungen bereit, einschließlich, aber nicht beschränkt auf Maßnahmen, die zur Lösung eines solchen Vorfalls ergriffen wurden, in gegenseitig vereinbarten Intervallen oder Zeiten für die Dauer des Vorfalls und so bald wie möglich nach Abschluss des Vorfalls , CWT einen schriftlichen Bericht vorzulegen, in dem der Vorfall, die vom Anbieter während seiner Reaktion ergriffenen Maßnahmen und die Pläne des Anbieters für zukünftige Maßnahmen beschrieben werden, um das Auftreten eines ähnlichen Vorfalls zu verhindern.

18.3 Einen solchen Verstoß gegen Informationen, Systeme oder andere Ressourcen von CWT nicht melden oder öffentlich offenlegen, ohne CWT vorher zu benachrichtigen und direkt mit CWT zusammenzuarbeiten, um zuständige regionale, landesweite, staatliche oder lokale Regierungsbeamte oder Kreditüberwachungsdienste, Personen, die von einem solchen Verstoß betroffen sind, zu benachrichtigen, und alle anwendbaren Medien, wie gesetzlich vorgeschrieben.

18.4 Ein Verfahren einrichten, um Verstöße gegen Sicherheitskontrollen, einschließlich der in diesen Informationssicherheitsanforderungen festgelegten, durch Mitarbeiter des Anbieters oder Dritte umgehend zu identifizieren. Identifizierte Zuwiderhandelnde unterliegen angemessenen Disziplinarmaßnahmen gemäß den geltenden Gesetzen. Ungeachtet des Vorstehenden bleiben Zuwiderhandelnde unter der Autorität des Anbieters oder seiner Drittparteien. CWT gilt nicht als Arbeitgeber des Lieferanten oder des Personals seiner Drittparteien .

19. Business Continuity Management und Disaster Recovery

Der Anbieter muss mindestens :

19.1 Entwickeln , betreiben, verwalten und überarbeiten Sie Business-Continuity-Pläne für jeden Standort und Disaster-Recovery-Pläne für jede Kerntechnologie, um die Auswirkungen von CWT auf den Service oder die Produkte des Anbieters zu minimieren. Diese Pläne müssen Folgendes umfassen: benannte Ressourcen, die für die Funktionen Business Continuity und Disaster Recovery spezifisch sind, festgelegte Wiederherstellungszeitziele und Wiederherstellungspunktziele, mindestens tägliche Sicherung von Daten und Systemen, Offsite-Speicherung der Daten und Systemsicherungen und -aufzeichnungen, Aufzeichnungen Schutz- und Notfallpläne gemäß den Anforderungen der Vereinbarung, bewahren Sie diese Aufzeichnungen und Pläne sicher außerhalb des Standorts auf und stellen Sie sicher, dass diese Pläne dem Anbieter bei Bedarf zur Verfügung stehen.

19.2 Stellen Sie CWT auf Anfrage einen dokumentierten Business-Continuity-Plan zur Verfügung, der sicherstellt, dass der Anbieter seine vertraglichen Verpflichtungen gemäß der Vereinbarung und diesem Dokument erfüllen kann , einschließlich der Anforderungen aller anwendbaren Leistungsbeschreibungen oder Service-Level-Vereinbarungen. Solche Pläne sollen eine Wiederherstellung durchführen und gleichzeitig die Integrität und Vertraulichkeit personenbezogener und vertraulicher Informationen schützen.

19.3 Dokumentierte Verfahren für die sichere Sicherung und Wiederherstellung personenbezogener Daten und vertraulicher Informationen, die mindestens Verfahren für den Transport, die Aufbewahrung und die Entsorgung der Sicherungskopien personenbezogener Daten und vertraulicher Informationen umfassen, und diese auf Anfrage von CWT zur Verfügung stellen dokumentierte Verfahren an CWT.

19.4 Stellen Sie sicher, dass mindestens einmal pro Woche Sicherungskopien aller gespeicherten personenbezogenen Daten und vertraulichen Informationen oder Software und Konfigurationen für von CWT verwendete Systeme erstellt werden.

19.5 Business-Continuity- und Disaster-Recovery-Pläne müssen mindestens einmal jährlich aktualisiert werden oder so oft, wie dies aufgrund wesentlicher Änderungen des Geschäfts- und/oder Technologieumfelds erforderlich ist.

19.6 Diese Pläne müssen auch nachvollziehbar mindestens jährlich oder nach jeder wesentlichen Änderung der Business-Continuity- oder Disaster-Recovery-Pläne auf alleinige Kosten und Kosten des Anbieters ausgeübt werden. Solche Übungen müssen das ordnungsgemäße Funktionieren der betroffenen Technologien und das interne Bewusstsein für solche Pläne sicherstellen.

19.7 - Plan, um zusätzliche oder neu auftretende Bedrohungsquellen oder -szenarien anzugehen, und stellen Sie CWT auf Anfrage innerhalb eines angemessenen Zeitrahmens eine allgemeine Zusammenfassung der Pläne und Tests zur Verfügung.

19.8 Stellen Sie sicher, dass alle Standorte des Anbieters oder des Anbieters, an denen personenbezogene Daten und vertrauliche Informationen von CWT aufbewahrt oder verarbeitet werden, 24 Stunden am Tag, sieben (7) Tage die Woche auf Einbruch, Feuer, Wasser und andere Umweltgefahren überwacht werden.

20. Compliance und Akkreditierungen

Der Anbieter muss mindestens :

20.1 Bewahren Sie vollständige und genaue Aufzeichnungen über die Erfüllung seiner Verpflichtungen aus diesen Informationssicherheitsanforderungen und deren Einhaltung durch den Anbieter in einem Format auf, das eine Bewertung oder Prüfung für einen Zeitraum von mindestens drei (3) Jahren oder länger, je nach Bedarf, ermöglicht aufgrund eines Gerichtsbeschlusses oder eines Zivil- oder Aufsichtsverfahrens. Ungeachtet des Vorstehenden ist der Anbieter nur verpflichtet, Sicherheitsprotokolle für mindestens ein (1) Jahr nach jeder fortgesetzten Erfüllung des Vertrags zu führen.

20.2 Erlauben Sie CWT, ohne zusätzliche Kosten für CWT, nach angemessener Vorankündigung, regelmäßige Sicherheitsbewertungen oder Audits der vom Anbieter verwendeten technischen und organisatorischen Sicherheitsmaßnahmen durchzuführen, wobei CWT dem Anbieter schriftliche Fragebögen und Unterlagen zur Verfügung stellt. Auf alle Anfragen antwortet der Anbieter mit einer schriftlichen Antwort und Nachweisen, falls zutreffend, unverzüglich oder nach gegenseitiger Vereinbarung. Auf Anfrage von CWT nach einer Prüfung durch CWT muss der Anbieter eine Sicherheitsprüfung ansetzen, die innerhalb von zehn (10) Werktagen nach einer solchen Anfrage beginnt. CWT kann Zugang zu Einrichtungen, Systemen, Prozessen oder Verfahren verlangen, um die Sicherheitskontrollumgebung des Anbieters zu bewerten.

20.3 Bestätigen Sie auf Anfrage von CWT die Einhaltung dieses Dokuments zusammen mit unterstützenden Zertifizierungen für die neuesten Versionen von PCI-DSS, ISO 27001/27002, SOC 2, Cyber Essentials oder einer ähnlichen Bewertung für den Anbieter und für jeden Subunternehmer oder Drittanbieter Verarbeitung, Zugriff, Speicherung oder Verwaltung im Auftrag des Anbieters. Wenn der Anbieter die Konformität nicht bescheinigen kann, muss er einen schriftlichen Bericht vorlegen, in dem detailliert aufgeführt ist, wo er nicht konform ist, und sein Abhilfeplan, um konform zu werden.

20.4 Für den Fall, dass CWT nach eigenem Ermessen der Ansicht ist, dass eine Sicherheitsverletzung aufgetreten ist, die CWT nicht in Übereinstimmung mit dieser Vereinbarung und dem Incident-Management-Prozess des Anbieters gemeldet wurde, planen Sie den Beginn des Audits oder der Bewertung innerhalb von vierundzwanzig (24) Stunden der Mitteilung von CWT, die eine Bewertung oder Prüfung erfordert.

20.5 Stellen Sie CWT innerhalb von dreißig (30) Kalendertagen nach Erhalt der Bewertungsergebnisse oder des Auditberichts einen schriftlichen Bericht zur Verfügung, in dem die Korrekturmaßnahmen aufgeführt sind, die der Anbieter implementiert hat oder umzusetzen gedenkt, mit dem Zeitplan und dem aktuellen Status jeder Korrekturmaßnahme.

Der Anbieter muss diesen Bericht alle dreißig (30) Kalendertage an CWT aktualisieren und den Status aller Korrekturmaßnahmen bis zum Datum der Implementierung melden. Der Anbieter muss alle Korrekturmaßnahmen innerhalb von neunzig (90) Tagen nach Erhalt des Bewertungs- oder Prüfberichts durch den Anbieter oder innerhalb eines alternativen Zeitraums umsetzen, sofern ein solcher alternativer Zeitraum von den Parteien innerhalb von höchstens dreißig (30) Tagen schriftlich vereinbart wurde. Tagen nach Eingang des Bewertungs- oder Auditberichts beim Lieferanten.

20.6 PCI-DSS-Konformität – Soweit der Anbieter Zahlungskontonummern oder andere zugehörige Zahlungsinformationen verarbeitet, muss der Anbieter derzeit die aktuellste Version von Payment Card Industry (PCI-DSS) für den gesamten Umfang der Systeme einhalten, die diese Informationen verarbeiten, und dies auch weiterhin tun solche Konformität. Wenn ein Subunternehmer oder Dritter Kreditkartendaten im Auftrag des Anbieters verarbeitet, auf sie zugreift, diese speichert oder verwaltet, sollte der Anbieter von diesem Subunternehmer oder Dritten ein PCI AOC erhalten und es CWT auf Anfrage zur Verfügung stellen. Für den Fall, dass der Anbieter den PCI-DSS für einen Teil des gesamten Umfangs der Systeme, die PCI-relevante Daten verarbeiten, nicht oder nicht mehr einhält, wird der Anbieter CWT unverzüglich benachrichtigen, umgehend und ohne unangemessene Verzögerung vorgehen, um diese Nichteinhaltung zu beheben, und bereitstellen den regulären Status einer solchen Behebung auf Anfrage an CWT weiter.

21. Standards, Best Practices, Vorschriften und Gesetze

oder vertrauliche Informationen von CWT-Mitarbeitern, Partnern, verbundenen Unternehmen oder CWT-Kunden verarbeitet, auf sie zugreift, diese anzeigt, speichert oder verwaltet ; oder Mitarbeiter, Auftragnehmer, Subunternehmer oder Lieferanten von CWT-Kunden ; Der Anbieter muss technische und organisatorische Sicherheitsmaßnahmen anwenden, die nicht weniger streng sind, als dies durch geltende globale, regionale, landesweite, staatliche und lokale Richtlinien, Vorschriften, Richtlinien und Gesetze erforderlich ist.

22. Änderung

Informationssicherheitsanforderungen von Zeit zu Zeit zu aktualisieren oder zu ändern , indem die neueste Version auf der Website von CWT veröffentlicht wird. Sofern der Anbieter solchen Aktualisierungen oder Änderungen nicht innerhalb von dreißig (30) Tagen nach der Veröffentlichung schriftlich widerspricht, gelten diese als vom Anbieter akzeptiert.

Version 6.1
Datum: April 2024